
Internal Revenue Service

# Privacy Updates Relevant to IRS System Development

*Richard W. Phillips*
*Associate Director,*
*Office of Privacy Compliance*
*Privacy, Information Protection & Data Security*

*June, 2010*

PIPDS
Privacy, Information Protection & Data Security

# Information Protection is on Everyone's Mind

"Recent GAO – TIGTA reports regarding lost laptops and other potentially damaging privacy incidents are impacting our relationships with Congress."

- *Washington Technology*

March 31, 2009

"The FTC also reports, 'About 90% of business record thefts involve payroll or employment records...'"

- Written Testimony of Commissioner before the Senate Finance Committee

April 12, 2009

"Since Americans have no choice in sharing their personal information with the IRS, the IRS has an obligation to ensure that its data security system is foolproof and that their privacy is protected."

- Excerpt from Senator Obama's Letter to

IRS Commissioner

April 9, 2007

# *Good News* – IRS Has an Excellent Reputation for Protecting Privacy

2008 survey of public regarding trust of Federal agencies:

IRS is 6th most trusted agency, at 70% affirmative

- The public's trust is a valuable asset, crucial to IRS mission
- Warning note:  VA's trust, following the "laptop incident," dropped from 75% affirmative to 34%

# Privacy and Security

- Privacy:  protection of public's and employee's **rights to privacy**
- Security:  protection of IRS assets, including information



***Significant overlap, though with different focus***

# Privacy and Information Protection Related Laws and Regulations


- **eGov Act of 2002:** To encourage use of electronic government by public. *Bolsters privacy protection*
- **IRC §6103:** Governs disclosure of tax data. *Tax data is confidential*
- **Privacy Act of 1974:** Fair Information Practices and confidentiality for Privacy Act records
- **Taxpayer Browsing Protection Act:** Privacy from unauthorized browsing of tax data
- **Federal Records Act:** Regulates agency records, including their disposition

## Upcoming Relevant Privacy Developments


- System Developers Privacy Training
- “Live Data for Testing” Management
- Privacy Tests within Security Test & Evaluation (ST&E)
- Privacy Impact Assessment updates
- Categorization of Personally Identifiable Information (PII)
- New Privacy Section Enterprise Architecture

# System Developer Privacy Training

**FISMA Training for Developers and others:**

***How to Build Privacy Protection into Systems***

- Will be targeted to system developers, or anyone with a role in protecting privacy within system design
- To be part of the FISMA Specialized Role-based Training
  - Will provide credits
- Expected roll-out October 2010

## “Live Data for Testing” Management

- OPC manages the approval for Live Data for Testing
  - Requests come to Live Data Mailbox
  - Must document there is no alternative to LD for these tests
    - Such as simulated or scrambled data
  - Project staff makes case to Approval Committee
    - Reps of PIPDS, TAD, Cyber Security, Data Strategy
  - Approval good for one year
- PIPDS assessing for better alternatives to be developed

## Privacy Tests for Systems

- Serve as check for system compliance with Enterprise Architecture
- Leverages current Security Tests and Evaluation (ST&E) process
- Shows follow-up on Privacy Impact Assessments
- Developing and piloting tests now with MITS AD staff
  - *Implementation TBD*

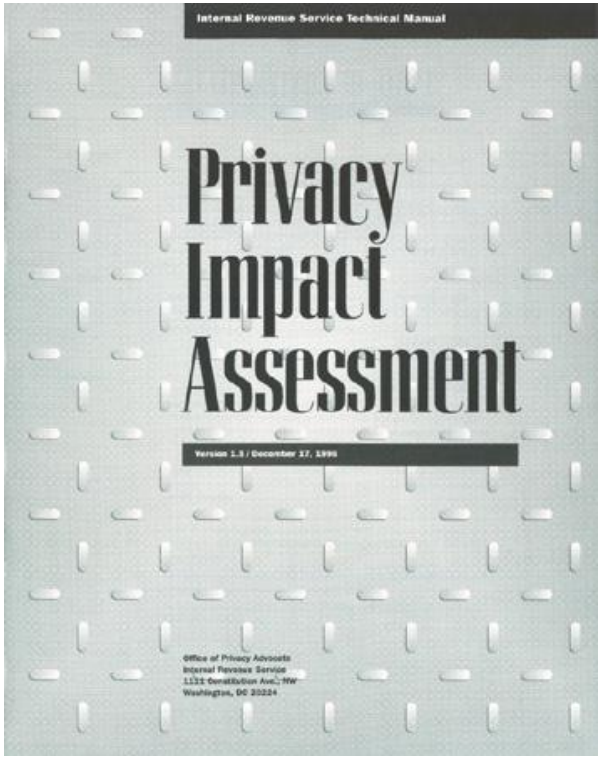
## New Privacy Impact Assessment (PIA) Template and Web-Based Management System

- New PIA template has been tested and approved
  - Now in publication and soon to be posted for Service implementation
- Ties directly to the privacy requirements of the Enterprise Architecture
- Working with Cyber on a Web-based PIA Management System
  - Automates creation, submission, tracking, and approval process
  - Implementation:  Fall 2010

# PIAs are a *Business Enabler*

PIAs:

- Ensure handling of personal information conforms to applicable legal, regulatory, and policy requirements regarding privacy
- Determine the risks and effects of collecting, maintaining and disseminating personal information in an electronic information system
- Assure the public that the Federal government is effectively managing *their* personal data
- Ensure that system owners understand their obligations regarding personal data



# Privacy Impact Assessments (PIAs) Federal Mandates

- The Electronic Government Act (eGov Act)
  - **IMPACT:** Encourage eGov by alleviating public's privacy concerns
- OMB Circular No. A-11: Preparation, Submission, and Execution of the Budget
  - **IMPACT:** PIA now basis for E-300 approvals
- NIST SP 800-53 Rev. 1 Recommended Security Controls for Federal Information Systems, February 28, 2006
  - **IMPACT:** PIA included in the Planning Security Controls
- Annual FISMA and Privacy Management Report and the President's Management Agenda
  - **IMPACT:** PIA metrics are a requirement

# Risk Assessments on Personally Identifiable Information (PII)

*Guide to Protecting Confidentiality of Personally Identifiable Information*

- NIST guidance published April 2010
- Requires categorization of PII based on systematic risk assessment
- Proposed risk factors include:
  - Identifiability:  license plate number vs. SSN
  - Sensitivity:  office phone # vs. criminal record
  - Context:  COTR training vs. alcoholism treatment
  - Legal requirements, e.g., IRC 6103
- Security then applied accordingly
- Waiting for instructions from OMB

## Revised Privacy Section for 2010 Enterprise Architecture

- Based on the Federal Architecture's *Privacy Profile*
- Expresses "privacy principles" to be built into systems
- Publication October 2010

# *What are these principles?*

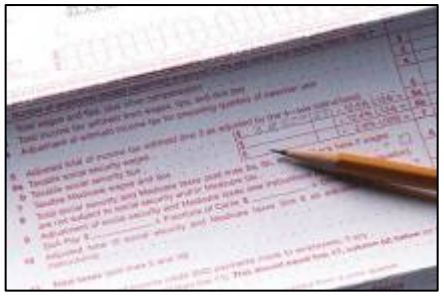
# How to Build Privacy Protection Into Systems – *These 8 privacy principles are filled out in the Enterprise Architecture*

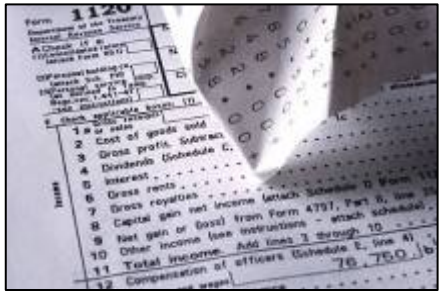
Build Your Systems To:

1. Collect Only Relevant Personal Data
2. Ensure Data Quality
3. Purpose of Personal Data Specified
4. Use Data Only for Purpose Collected
5. Protect Data
6. Public Awareness
7. Allow the Public to Access, Correct Data
8. Accountable to the Public

# How to Build Privacy Protection Into Systems

1. Collect Only Relevant Personal Data:
   - Limit the collection of personal data; where appropriate, with consent or knowledge of subjects
   - In system design:
     - Collected data must be relevant to the system's purpose
     - Design system to only collect what is required
     - Disable unneeded features regarding collection
2. Ensure Data Quality:
   - Personal data must be accurate, complete, current, and verified
   - In system design:
     - Establish automated checks to ensure completeness, accuracy, timeliness
     - Perform inter-system cross-checks
     - Provide means for correction
     - Audit logs on changes





# How to Build Privacy Protection Into Systems

3. Purpose of Personal Data Specified:
   - Purpose must be specified in writing
   - Use must be limited to purposes stated
   - In system design: Design enforces system purpose, especially in relation to use of personal data


4. Use Data Only for Purpose Collected:
   - Use or disclosure limited to Principle #3, except where consent is provided or required by law
   - In system design:
     - Technology deployed to restrict use, disclosure
     - Mitigate risks from interconnections
     - Mask unneeded identifiers
     - Enable audit logs to track usage

# How to Build Privacy Protection Into Systems

5. **Protect Data:**
   - Safeguard data against loss, destruction, modification, use except as authorized
   - In system design:
     - Systems with PII properly classified as sensitive, with appropriate cyber, physical, and personnel security
     - Check on safeguard responsibilities in sharing agreements
     - Know and follow your Records Control Schedule (RCS) in the archiving and disposal of records

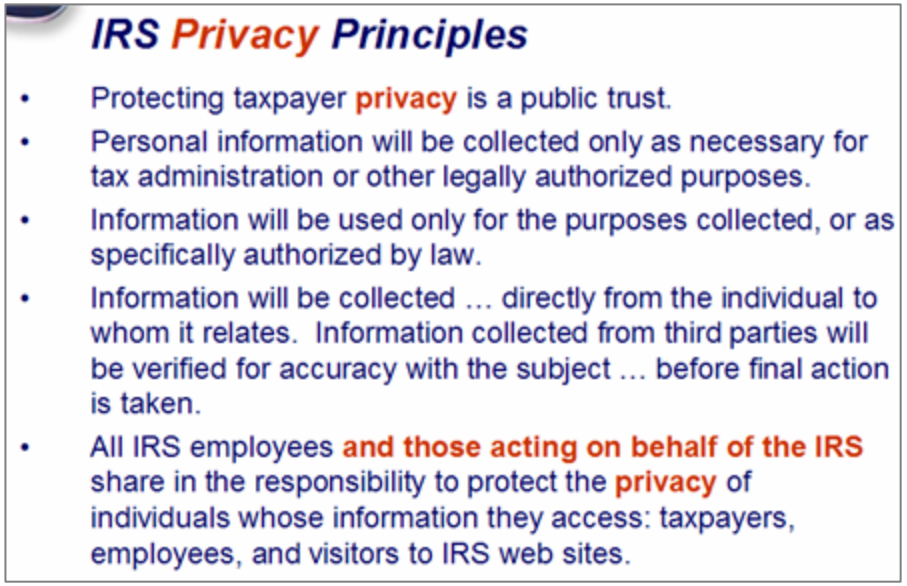
6. **Transparency:**
   - Collection, use, and maintenance of personal data should be open to the public as much as appropriate – *transparency*
   - In system design:
     - Verify PIAs and SORNs and keep up-to-date
     - Permit oversight, audit accountability
     - Web pages must have conforming privacy statements, as well as cite legal authority to collect SSN and other private information

# How to Build Privacy Protection Into Systems

7. **Allow the Public to Access, Correct Data:**
   - Individuals have the right to know what information is held about them, get copies, get corrected, and can challenge denials
   - In system design: Provide the capability to correct data per public's requests

# How to Build Privacy Protection Into Systems

8. **Accountable to the Public:**
   - Data stewards are accountable for protecting privacy
   - In system design, someone is responsible to ensure
     - Privacy principles are included
     - Protections are documented, tested, and implemented
     - System changes preserve and enhance privacy protections



# Your Privacy Responsibilities

Whether you are an IRS employee or contractor, you have access to very sensitive information – the tax, financial, and personal information of our citizens and taxpayers.

- All IRS data is sensitive
- It is personal information about real people
- Fragments or part of a record are still treated as sensitive
- You may use this data only for the reason it was collected
- Treat it as if it were your own!
- Follow accountability practices and procedures
- Disclose/share only on a “need to know”
- Request and use only the information you need
- Limit access to the data you have
- Dispose of the data per IRS procedures
- Ensure you—and your coworkers—comply with these requirements
- Report suspected privacy breaches

# Resource Web Sites

## Office of Privacy Compliance

http://irweb.irs.gov/AboutIRS/bu/pipds/default.aspx

## Governmental Liaison and Disclosure

mysbse.web.irs.gov/CLD/GLD/Disclosure/Office/default.aspx

## Office of Records Management

http://awss.web.irs.gov/facilities/RecordsMgmt/REFM-Index.htm